AO 106 (Rev. 7/87) Affidavit for Search Warrant

REDACTED

United States District Court

DISTRICT OF DELAWARE

REDACTED

In the Matter of the Search of

(Name, address or brief description of person, property or premises to be searched)

[redacted]
Dover Air Force Base, Delaware 19902,
described more particularly on
Attachment A

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 07- 167M-

I Michael Deshaies being duly sworn depose and say:

I am a(n) Immigration and Customs Enforcement Special Agent and have reason to believe
Official Title

that ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

[redacted] Dover Air Force Base, Delaware 19902, described more particularly on Attachment A

in the _____ District of Delaware

there is now concealed a certain person or property, namely (describe the person or property to be seized)

described in Attachment B

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

evidence of a crime and contraband

concerning a violation of Title 18 United States code, Section(s) 2252 and 2252A.

The facts to support a finding of Probable Cause are as follows:

Affidavit attached.

FILED
OCT 24 2007
U.S. DISTRICT COURT
DISTRICT OF DELAWARE

Continued on the attached sheet and made a part hereof. ☒ Yes ☐ No

Michael J. Deshaies
Signature of Affiant
Michael Deshaies
Special Agent, Immigration & Customs Enforcement

Sworn to before me, and subscribed in my presence

August 27, 2007 at Wilmington, Delaware
Date City and State

Honorable Leonard P. Stark

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED:

The subject premises is a dormitory room, Room [redacted] located in Building [redacted] on [redacted] Dover Air Force Base, Delaware. Room [redacted] is located on the northwest side of Building [redacted] on the second floor. The door to Room [redacted] is brown and is labeled with a sign that reads "[redacted] AMXS, AIC Gramlich, Day Sleeper" in white letters. The door knob is located on the right side of the door and the door hinges on the left. There is one window to the right of the door.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED FOR AND SEIZED

a. images of child pornography and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:

i. any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, aud other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

iv. motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

b. information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

c. credit card information including but not limited to bills and payment records;

d. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

e. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access including Comcast Cable Communication, and handwritten notes.

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE SEARCH)
OF THE RESIDENCE LOCATED AT:)
)
[redacted])
Dover Air Force Base, Delaware 19902)

AFFIDAVIT

I, Michael J. Deshaies, being duly sworn, depose and state the following:

1. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), assigned to the Resident Agent in Charge office in Wilmington, Delaware. I have been employed as a Special Agent since October 01, 1997, when the INS employed me. The INS investigations branch was transferred to the U.S. Department of Homeland Security as Immigration and Customs Enforcement ("ICE") in March 2003. As part of my official duties as an ICE agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. This affidavit is submitted in support of an application for a search warrant for the residence located [redacted] Dover Air Force Base, Delaware (Subject Premises), and the computer(s) located therein, for evidence of violations of Title 18, United States Code, Sections 2252 and 2252A. The Subject Premises is more fully described in Attachment A. I am

familiar with the information contained in this Affidavit based upon the investigation I have conducted and based on my conversations with other law enforcement officers who have engaged in this and numerous other investigations involving child pornography.

3. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2252 and 2252A is presently located at the Subject Premises.

Relevant Statutes

4. This investigation concerns alleged violations of 18 U.S.C. Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors.

5. 18 U.S.C. Sections 2252 and 2252A prohibit a person from knowingly transporting, receiving, distributing or possessing in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct (child pornography).

Definitions

6. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

7. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

8. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

9. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

10. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

11. "Internet Service Providers" or "ISPs" are commercial organizations, which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

12. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters,

with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the world wide web server located at the United States Department of Justice, which is part of the United States government.

13. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

14. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

15. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

16. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website

is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

17. The terms "records", "documents", and "materials", as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Background Regarding Seizure of Computers

18. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following:

19. Computer storage devices (like hard drives, diskettes, tapes, laser disks, Bernoulli drives and others) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

20. Searching computer systems for criminal evidence is a highly technical process requiring expert skills in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

21. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly

requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

22. In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem and other system components were used as a means of committing offenses involving the sexual exploitation of minors in violation of law, and should all be seized on that basis alone. Accordingly, permission is sought herein to seize and search computers and related devices consistent with the scope of the requested search.

Background Regarding the Internet

23. I have been trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet since 1993. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

24. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an

IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

25. Photographs and other images can be used to create data that can be stored in a computer. This storage can be accomplished using a "scanner", which is an optical device that can recognize characters on paper and, by using specialized software, convert them to digital form. Storage can also be captured from single frames of video and converted to an image file. After the photograph or other image has been scanned into the computer, the computer can store the data from the image as an individual "file". Such a file is known an image file. Computers are capable of displaying an image file as a facsimile of the original image on a computer screen.

26. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a

video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

27. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading". The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and or print out a hard copy of the image by using a printer device (such as a laserjet or inkjet).

28. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an

electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

Background of Investigation

29. Your Affiant can state that peer to peer networks are frequently used in the distribution of child pornography. In particular, one network known as the Gnutella network is being used to trade digital files, including still image and movie files of child pornography. Your Affiant can state the following about the operation of the Gnutella file-sharing network:

a. Gnutella is a decentralized, server-based, **peer-to-peer file sharing** network used primarily to exchange audio files, video files and computer software. Like most file sharing networks, it is decentralized; files are not stored on a central server but are exchanged directly between "Peers" (Users).

b. Indexing computers referred to as "Ultra-Peers" increase the efficiency of the Gnutella network by maintaining an index of the contents of peers.

c. Computers using the Gnutella network have software installed on them that facilitates the trading of files and images. The software, allows the user to search for pictures, movies and other digital files by entering certain text as search terms.

d. The search results presented to the user allow them to select a file and then receive that file from other users (peers) around the world. Often, users can receive parts of the selected digital file from numerous sources at once.

e. The Gnutella client software balances the network load and recovers from network failures by accepting parts of the digital file from different users and then reassembling the digital file when it reaches the requesting local computer.

f. Gnutella network can only be successful in reassembling the digital file from different parts if the parts all come from the exact same digital file. Gnutella uses SHA1 or Secure Hash Algorithm Version 1 to ensure exact copies of the same file.

g. Secure Hash Algorithm Version 1 is a file encryption method which may be used to produce a unique digital signature of a file. This method was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard. The SHA-1 value assigned to any file or image is unique; therefore, merely locating a file or image by the SHA-1 value assigned, without looking at the file or opening it, and irrespective of the file name or title, allows identifying the content of a particular file. Explained another way, digital files can be processed and identified by this SHA-1 process resulting in a digital signature or fingerprint.

h. Entering search terms in the Gnutella software returns a list of files and descriptive information including SHA1 signatures. By using this type of search your law enforcement officers can compare the offered SHA1 signatures with SHA1 signatures known to belong to movies or images of known child pornography. Once a matching set of digital signatures was identified, the officers could use publicly available software to request a list of Internet network computers that are reported to have the same images for trade or are participating in the trade of known images. This feature allows officers to conduct undercover operations that involve images known to be actual and identified child pornography involving identified children.

i. Your Affiant knows from training and experience that computers connected to the Internet identify each other by an Internet Protocol or IP address. IP addresses can assist law

enforcement in finding a particular computer on the Internet. These IP addresses can typically lead the law enforcement officer to a particular Internet service company and that company can typically identify the account that uses the address to access the Internet.

j. Searching on the Gnutella peer to peer network as described above results in the user receiving a list of IP addresses identifying specific computers that have the Gnutella software installed, and where the computer user has placed files with a specific digital signature into an open folder and made them available for downloading by others.

k. Your Affiant knows that the IP address can be used to identify the location of these computers. The ability to identify the approximate location of these IP address is provided by IP geographic mapping services, which are publicly available and also used for marketing and fraud detection.

l. By examining the list of IP addresses, law enforcement officer can locate computers that are reported to be in Delaware. By comparing the SHA-1 digital signatures, officers can conclude that a computer, originating from an IP address known to be in Delaware, has Gnutella or compatible software installed on it and contains specific and known images or videos of child pornography.

Investigation

30. On August 7, 2007 at approximately 1700 hours Det. Ronald Garland of the Delaware State Police High Technology Crimes Unit conducted an undercover Internet investigation into the distribution and receipt of child pornography via file peer to peer file sharing networks. Det. Garland located a computer offering to share a video file known to contain child pornography. The file titled: [redacted]". Det. Garland was presented

with an IP address of 71.204.215.215. Det. Garland was able to determine that the IP address was identified to an Internet Service provide in Delaware.

31. Det. Garland was able to browse the publicly available shared file directory of the computer associated with IP 71.204.215.215. A total of 603 files were being shared and based on the titles, several files within this directory appeared to be pornographic movie files depicting minors engaged in prohibited sexual acts. A listing of the files and verification of a connection between the investigative computer and the suspect computer, Netstat log, was preserved for evidentiary purposes. The log establishes those files were present on the suspect computer at that time.

32. Det. Garland compared the 603 files unique SHA-1 values found on the computer associated with IP 71.204.215.215 with previously identified child pornography. Det. Garland determined that 103 files of the files were of known child pornography.

33. Your Affiant can state that known child pornography or suspected images of child pornography are catalogued by the National Center for Missing and Exploited Children (NCMEC) and/or the Wyoming Internet Crimes Against Children Task Force. To be considered as "known child pornography" and be a part of this database, the image is either one in which the child victim is actually known to law enforcement and catalogued by NCMEC, or the image has been viewed by other members of law enforcement who are able to confirm by training and experience that the content is child pornography, as defined in 18 U.S.C. § 2256(8), the child depicted is a real child.

34. On August 8, 2007 a WHOIS inquiry on IP addresses 71.204.215.215 and found it to be issued to a subscriber with Comcast Cable Communications.

35. On August 9, 2007 Det Mathew Zolper of the Delaware State Police High Technology Crimes Unit requested and received a Delaware subpoena, directing Comcast Cable Communications to supply subscriber information as well as Internet connection access logs for the

person assigned/using the IP address 71.204.215.215 on August 7, 2007, at the specific hour, minute and second of Det. Garland's contact with that IP address.

36. On August 20, 2007, your Det. Zolper received a response from Comcast Cable Communications indicating that one account had been accessing/using the IP address on the given date and specified time. The account contained the following information:

Name:	John Gramlich
Address:	[redacted] Dover De 19902
Account Status:	Active

37. Your Affiant can state that investigation revealed that [redacted] Dover DE is located on Dover Air Forces Base.

38. On August 21, 2007 SA Amber R. Armbruster, Dover Air Force Base OSI stated that she had examined the administrative records of John Gramlich. The records revealed contained the following information:

Name:	John Gramlich
Address:	[redacted] Dover AFB, De 19902
DOB:	[redacted]
Race:	White
SEX:	Male
Hair:	Brown
Eyes:	Blue
Height:	5'10
Weight:	201

39. On May 10, 2006, a U.S. Air Force Assistant First Sergeant performed a no-notice monthly room inspection on the Subject Premises, which resulted in a letter of reprimand for excess trash to John Gramlich on May 10, 2006. During the course of the no-notice monthly room inspection, several photographs of the Subject Premises were taken by the inspector. One of the photographs depicts a computer monitor and keyboard. The photographs also seems to depict a computer mouse and CPU tower, but the picture is too blurred to be certain.

Conclusion

40. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the residence described in Attachment A, in violation of 18 U.S.C. §§ 2252 and 2252A.

41. I, therefore, respectfully request that attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Michael J. Deshaies

Special Agent Michael J. Deshaies
Immigration & Customs Enforcement

SUBSCRIBED and SWORN before
me this 27th of 2007

Leonard P. Stark

HONORABLE LEONARD P. STARK
United States Magistrate Judge